CRS Insights

Information Warfare: The Role of Social Media in Conflict

Catherine A. Theohary, Specialist in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844)

March 4, 2015 (IN10240)

Social media is used as a tool of information warfare—a weapon of words that influences the hearts and minds of a target audience, and a weapon of mass disruption that can have effects on targets in the physical world. Low-cost, easily accessible social media tools act as a force multiplier by increasing networking and organizing capabilities. The ability to rapidly disseminate graphic images and ideas to shape the public narrative transforms social media into a strategic weapon in the hands of terrorists, insurgent groups, or governments engaged in conflict.

Facebook, Twitter, YouTube, blogs, and a host of other social media applications are used by terrorist organizations to identify, radicalize, and recruit new warriors; provide training tools and resources for the radicalized; raise money; publicize successes; and shape public perception regarding ongoing hostilities. Al-Qaeda has a media apparatus that distributes video and graphic products online through jihadist forums, blogs, and dedicated file-hosting websites. These websites can also carry comprehensive instructions on how to build and detonate bombs. Some websites are said to carry a downloadable "e-jihad" application, through which a user can choose an Internet target and launch a low-level denial of service cyberattack. Social networking tools can also aid in providing material support for planned acts of terrorism, as well as for target acquisition through intelligence, surveillance, and reconnaissance.

The Islamic State (IS) has used social media to reach a wide audience. In January 2015, a group claiming to be IS sympathizers called CyberCaliphate hacked the Twitter account of the U.S. Central Command. Although the group was posting materials that were already publicly available, the hacking created the perception that the U.S. military's accounts were vulnerable. Twitter subsequently retaliated by suspending approximately 2,000 accounts said to be linked to IS and its supporters, many of whom were major distributors in the organization's campaign against the U.S. military's own information operations (IO). An information operation is the military term for the employment of information-related capabilities to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries.

In addition to the use of social media as a cognitive weapon, there are concerns about terrorist groups or hostile nation states obtaining the ability to use the Internet to launch an attack on a physical target. The successful deployment of the Stuxnet worm, a malicious software of unknown origin that was used to attack centrifuges in Iranian nuclear facilities, has raised questions on whether a terrorist group may be able to develop a similar cyber weapon. Terrorists could employ the Internet and social media to study the Stuxnet code and tailor it to attack computers that control critical infrastructure and commerce.

Social media can be also used by governments to spread a public diplomacy message and to aid pro-democracy (or authoritarian) movements abroad. Yet these activities contain an inherent risk in that support for government policies and operations erodes when those same tools rapidly proliferate stories and images that reveal classified information or reflect negatively on the government. Messaging where government sponsorship is known may be less effective if it is perceived by the target audience as government propaganda lacking in credibility.

The ongoing conflict between Ukraine and Russia illustrates the role of social media in achieving multiple objectives. Ukrainian government networks have been targets of cyberattacks that may have been coordinated by "patriotic hackers" using social media tools to organize, train, and equip themselves. Spyware was discovered on Ukrainian government systems that was believed to have been developed in Russia. The Russian government has used the blogosphere to control the narrative of the conflict, allegedly by mobilizing hacker collectives and encouraging them to maintain several accounts and to post and comment on multiple social media outlets per day. Both sides have attempted to exercise control over the information environment. Recent legislation was introduced in Ukraine that would have criminalized publicly criticizing the government, while another bill proposed amendments to the Law on Information that would impose regulations on bloggers, including establishing rules and duties. A Russian law approved in August 2012 compels bloggers with more than 3,000 followers to register their activity with the government.

The body of law governing this relatively new space can be ambiguous, leading some to characterize it as the ungoverned "Wild West." Questions of territorial sovereignty arise due to the interconnected, globalized nature of the Internet. Much of the available information and communications technology is owned by private sector companies and operates outside of the control of governments. Many social media providers have terms of use that prohibit publishing web pages that promote or depict terrorist violence. These user agreements often rely on self-policing mechanisms, whereby users flag content they deem to be "inappropriate." However, an individual's content may be covered by free speech and anti-censorship protections. Flagging material as inappropriate, in turn, can be an attack launched by those with opposing interests.

In the United States, media reports have suggested that the Department of Homeland Security has established a number of programs to monitor and analyze information contained in various social media websites, while the Department of Defense and the National Security Agency may have exercised offensive cyber activities to dismantle some sites. Federal efforts to assess a combatant's use of social media require cost/benefit analysis of a site's intelligence value versus the operational threat it presents. A terrorist group's or individual's website may present such a risk that it would be necessary to dismantle it through a cyberattack. However, this could lead to unintended consequences as an attack on a host server could have cascading effects throughout a network. In addition, efforts to take down websites may prove futile as the websites can easily pop up on new servers, a phenomenon referred to by security observers as "whack-a-mole." On the other hand, government agencies may wish to keep a website or application operational for surveillance and intelligence gathering purposes. The military or intelligence community may also use offensive cyber operations in order to gain control of a platform for use in disseminating counterintelligence or strategic communications. An added effect of this approach would be to create fear and doubt in the minds of the users, who could not be certain that their communications were secure.